A Parallelism-Based Approach to Network Anonymization

Igor Margasiński

Institute of Telecommunications, Warsaw University of Technology
igor@tele.pw.edu.pl

Abstract. Considering topologies of anonymous networks we used to organizing anonymous communication into hard to trace paths hiding its origin or destination. In anonymity the company is crucial, however the serial transportation imposes a costly tradeoff between a level of privacy and a speed of communication.
This paper introduces a framework of a novel architecture for anonymous networks that hides initiators of communications by parallelization of anonymous links. The new approach, which is based on the grounds of the anonymous P2P network called P2Priv, does not require content forwarding via a chain of proxy nodes to assure high degree of anonymity. Contrary to P2Priv, the new architecture can be suited to anonymization of various network communications, including anonymous access to distributed as well as client-server services. In particular, it can be considered as an anonymization platform for these network applications where both privacy and low delays are required.

Key words: Communication system security, privacy, anonymity

1 Introduction

Anonymous communications by means of public packet networks involve two contradictory tasks: the first is **transport and routing**—which requires a detail information on origin and destination points of communications, and the second is **anonymization**—which is basically aimed at hiding of this information and especially an association between them. Certainly, addressing information is essential for a successful delivery of content and therefore it cannot be expunged. Hence in general, the ally of anonymous communication is collective [10,7,8]. The single word *crowd* speaks volumes about anonymity. The more numerous a set of actors involved in an information exchange *blending into a crowd* is easier to achieve. And then, the higher traffic volume among these actors the faster our traffic can be hidden and exchanged. In general, to represent such a collective, an operation of anonymous networks is based on a sequential traffic forwarding by a subgroup of network nodes, also known as *proxy chaining* [13]. However, substantial delays mount up in this way. This paper introduces an alternate architecture for anonymous networks, a network privacy preserving parallel topology, where network actors organize themselves in parallel links.

The topology of the new solution evolves from the anonymous P2P network called P2Priv [16]. However, the applications of the new architecture are not limited to P2P content distribution and its deployment can be considered for generic-purpose anonymous networks.

The rest of the paper is organized as follows. Section 2 provides an introduction to topology issues of anonymous networks. Section 3 describes a model of an adversary while Section 4 contains an anonymity analysis of parallel architecture of P2Priv applied first, in accordance with its intended use, for P2P content distribution, and secondly, for client-server like scenarios. Section 5 contains a description of our novel solution able to assure anonymity for centralized network services, while its anonymity analysis is presented in Section 6. Conclusions and discussion of a future work are included in Section 7.

2 Background

The topology of anonymous networks has been widely discussed since the introduction of Chaum's Mix-net anonymous network [4] and among a variety of anonymous networks, the most attention has been devoted to the interconnection issues of Mix-based nodes. Originally, the route through a cascade of Mixes was fixed. Further improvements allowed a sender to randomly select a path for each message in the so called free-route topologies [1,12]. Hybrid models with a restricted number of connections and path selection narrowed to restricted-routes were proposed in [6]. Both fixed cascades and fully interconnected Mix networks with random routes have assorted constraints and the advantage of each depends primarily on the area of their deployment and the scale of the network [1,2,5,14]. Today's Mixes allow to route content in various ways determined by sender nodes.

Besides Mixes, other designs of anonymous networks were proposed within individual interconnection strategies. Anonymous message-by-message routing called *onion routing* was proposed by Goldschlag et al. [13]. Today, several implementations of this concept are available, including the low-latency network called *the second generation onion router* (TOR) designed by Dingledine et al. [11]—the general purpose anonymous network of the world-wide range.

Reiter et al. proposed other low-latency anonymous network called *Crowds* with anonymous routing based on the *rando-walk* step [18]. In this strategy senders do not influence a path selection which is determined in a random manner in each hop sequentially. Both hop-by-hop and message-by-message routing strategies are less robust against traffic dropping by proxy nodes than Mix-network. Still, their simplicity makes them attractive in practice [3].

By and large, the common feature of anonymous networks is their **serial** architecture and a formation of untraceable paths via middle-man nodes for anonymous content forwarding. Due to such praxis, and in combination with traffic encryption and anonymization techniques deployed inside proxy nodes (e.g., content batching, aggregations, and permutations), an observer of the anonymous networks cannot practically point out senders and receivers in a batch of intermixed content flows via middle-man nodes.

2.1 Parallel Architecture of P2Priv

The serial content forwarding, known from today's anonymous networks, was omitted in the architecture of the anonymous peer-to-peer overlay network called P2Priv (peer-to-peer direct and anonymous distribution overlay) proposed by Margasiński et al. in [16]. The topology of the P2Priv network, in respect to content transportation, involves a number of additional virtual links similar to classical anonymous networks; however it is arranged in a **parallel** manner. Figure 1 illustrates the parallel architecture of P2Priv with solid lines representing plain-text communication and dotted lines corresponding to communication secured by the anonymization techniques. Let us have a closer look at the P2Priv architecture. Before a content transportation, a signalization token with meta-data describing the content is forwarded over classical anonymous paths towards formation of so called *cloning cascades* (CC). The well-known anonymous techniques (i.e., Mix network and random walk algorithm) are utilized in the anonymization process of this *lightweight* communication (traffic comprised by numerous and short messages sent by random nodes is in favour of a Mix-net performance) and hiding the initiator of the CC. Then, after a random interval of time, each CC member (i.e., group of the so called *clones* and the true initiator) communicates directly and independently with a destination node or nodes towards content transportation. The anonymity of P2Priv is based on a collective formed in a parallelism-based manner, as every content exchange in P2Priv is accompanied by a simultaneously generated exchange of the same content between random nodes. The process of finding the true initiator among P2Priv nodes is hard to perform even for an adversary able to collude a significant range of nodes.

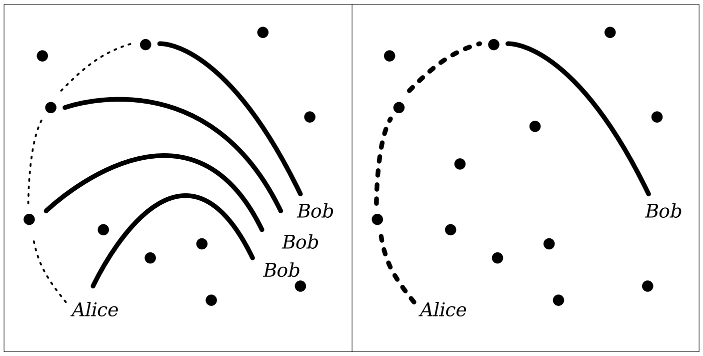


Fig. 1: P2Priv architecture (*left*) as compared to classical anonymous network (*right*).

Results of anonymity and traffic performance analysis are promising for P2Priv [16,17]. However, they have been obtained for a distributed environment which is not always available in general-purpose communications.

3 Threat Model

We consider a threat model with a partial adversary who controls a colluding fraction ρ of all overlay network nodes N. These malicious nodes are able to provide both passive and active attacks. We consider a static adversary unable to arbitrarily adapt the set of malicious nodes among user nodes and we assume that colluding nodes are uniformly distributed among equivalent nodes. However, whenever we will deal with server-like nodes or just centralized points of communication, we will treat these nodes as easy to choose points of observation and assume that these nodes can be compromised. Using information entropy measures and based on the information theoretic anonymity measurement model [9,19], an adversary who posses no information about the system can describe his/her uncertainty in successful finding of the initiator of a particular action (let as call her *Alice*) as

$$\begin{aligned}\mathcal{H}_{\max} &= -\sum_{i=1}^{|N|(1-C_s)} \frac{1}{|N|\,(1-\rho)} \log_2\left(\frac{1}{|N|\,(1-\rho)}\right). \\ &= -\log_2(|N|\,(1-\rho)).\end{aligned} \tag{1}$$

4 Anonymity Analysis for P2Priv

As the new architecture proposed in this paper share some primitives with P2Priv, we will apply the threat model to P2Priv architecture first and discuss its anonymity in two service scenarios. In the first one, likely to occur in fully distributed P2P systems, we will consider content distribution (e.g., P2P file-sharing) among equivalent peers. Secondly, we will analyze anonymity offered by P2Priv for typical client-server network services where client nodes connect repeatedly to some server (e.g., a popular Web server). Notice that models, similar to the first scenario, has been investigated previously in [16,15,17] with different adversary possibilities considered. The second scenario has not been considered yet. For simplicity purposes, the scenarios will be referred to as **P2P Scenario** and **Client-Server Scenario** respectively.

The detailed description of P2Priv was introduced in[17]. At a glance, cloning cascade (CC) of P2Priv is established in random-walk manner with a mean length described by probability p_f, as follows [17]

$$|CC| = \frac{p_f - 2}{p_f - 1}. \tag{2}$$

Each step of the token's random-walk is sent by a Mix-network layer formed for this purpose by user nodes (N). After establishing CC, randomly delayed direct connections originate from CC nodes towards content transportation (Figure 1). The analysis of various attacks on P2Priv (presented in [15]) shows that a secure configuration of P2Priv starts from $p_f = 2/3$ which corresponds to CC mean length equal 4.

4.1 P2Priv in P2P Scenario

The adversary tries to find out who initiates a content distribution in respect to some content of his interest. A linkage between the cloning token's sender—*Alice* and the cloning token is hidden by means of the Mix-net layer. Mix-net is recognized as one of the strongest anonymization methods. However, it requires adequate user traffic characteristics to achieve its best results. In particular, traffic volume is crucial for its efficiency. Daz *et al.* in [8] prove that practical Mix designs achieve results close to perfect indistinguishability for high traffic arrivals. For each P2Priv transaction, the P2Priv protocol generates short but numerous messages sent by random nodes. This can allow Mix-net to assure high anonymity without unnecessary delays. The anonymity analysis of Mix-net is independent of the current exposition and in our model we assume perfect performance of Mix-net layer. We assume that the adversary does not get any information about *Alice* during the establishment of CC. However, the adversary having the fraction ρ of malicious nodes can gain awareness that a particular content is about to be distributed. If the cloning token describing this content is passed via one of the malicious nodes, the adversary can disturb CC establishing in a way that allows him to get more information in a subsequent phrase of content transportation. The adversary, who looks for the initiator of particular content's distribution, can try to narrow the circle of suspects. While possessing fraction ρ of colluding nodes among N, he/she can break the cloning cascade using the first malicious node which intercepts the cloning token. The probability that the adversary manages to break CC immediately after sending out the token by *Alice* equals $\Pr(|CC_{break}| = 1) = \rho$ (we assume that colluding nodes are uniformly distributed among N). The length of random-walk is one more hop longer with probability $\Pr(|CC_{break}| = 2) = (1-\rho)(p_f\,\rho + (1-p_f))$. Then

$$\Pr(|CC_{break}| = n) = (1-\rho)^{n-1}(p_f^{n-1}\,\rho + (1-p_f)p_f^{n-2}). \tag{3}$$

As a result of this action the adversary concludes that the set of parallel connections associated with the interesting content exchange will contain an average of $|CC_{break}|$ links, where

$$|CC_{break}| = \rho + \sum_{i=2}^{|CC|} i(1-\rho)^{i-1}(p_f^{i-1}\,\rho + (1-p_f)p_f^{i-2}) =$$
$$[\ (1+|CC|){p_f}^{|CC|}(\rho-1)^{|CC|} -$$

$$\begin{aligned}&|CC|\, {p_f}^{|CC|+1}(\rho-1)^{|CC|+1} - \\ &p_f(\rho-2)+{p_f}^2(\rho-1)\ ] \\ &p_f(1+p_f(\rho-1))^{-1}, |CC_{break}| \leq |N|(1\text{-}\rho).\end{aligned} \tag{4}$$

After establishing of CC, P2Priv protocol starts direct, plain-text connections from CC members to destination nodes with shared content, each independently delayed with a random interval of time. In the analyzed P2P Scenario the content is shared between equivalent peers N. Then, having in mind the considered threat model, we assume that malicious nodes are also uniformly distributed among destination nodes. The adversary managed to reduce the cloning cascade from mean length equal $|CC|$ to $|CC_{break}|$ (4). Next, he/she will eavesdrop on each content connection established to $\rho\,|N|$ colluded nodes in order to detect transmission of the content of his/her interest and in consequence in search of connected CC_{break} members. It immediately follows that the adversary is able to identify $CC_{eavesdrop}$ peers connected towards the particular content transportation, an average of

$$|CC_{eavesdrop}| = \rho\,|CC_{break}|\,. \tag{5}$$

Until he/she can be certain that $CC_{eavesdrop}$ includes all of the CC or CC_{break} members, he/she cannot be determine that $CC_{eavesdrop}$ set includes *Alice*. Let us estimate the uncertainty of the adversary in linking of the found traces to the real initiator. Each $CC_{eavesdrop_k}$, $k = \{1, \ldots, |CC_{eavesdrop}|\}$ node can be *Alice,* with equal probability

$$p_{a1} = \Pr(CC_{eavesdrop_k} = Alice) = |CC_{break}|^{-1}\,. \tag{6}$$

Alice also can be outside eavesdropped nodes and can be each other honest node of the network in the number of $|N| - \rho\,|N| - |CC_{eavesdrop}|$. The attack conducted by the adversary allows him/her to assign probability that one of this nodes is *Alice*, to each equal

$$p_{a2} = \frac{1-p_{a1}}{|N| - \rho\,|N| - |CC_{eavesdrop}|}. \tag{7}$$

Then, we can stress the entropy of P2Priv in P2P Scenario as the following sum of two components corresponding to the set of nodes managed to have been eavesdropped by the adversary and the rest of nodes, respectively

$$\begin{aligned}\mathcal{H}_{\mathrm{p2priv/p2p}} = &-\sum_{k=1}^{|CC_{eavesdrop}|} p_{a1}\log_2(p_{a1}) \\ &-\sum_{l=1}^{|N|-\rho\,|N|-|CC_{eavesdrop}|} p_{a2}\log_2(p_{a2}).\end{aligned} \tag{8}$$

Finally, after substitution and simplification we will then get

$$\begin{aligned}\mathcal{H}_{\mathrm{p2priv/p2p}} = {} & \frac{|CC_{eavesdrop}|}{|CC_{break}|}\log_2(|CC_{break}|) - \\ & \frac{1-|CC_{eavesdrop}|}{|CC_{break}|}\log_2(\frac{1-|CC_{break}|}{|N|-\rho\ |N|-|CC_{eavesdrop}|}). \end{aligned} \tag{9}$$

Figure 2 shows entropy of P2Priv architecture as applied to distributed P2P file-sharing service. The entropy of small network ($|N| = 10$) is plotted in the full spectrum of colluding nodes. The presented results were obtained for P2Priv in the following configurations $p_f = \{1/2, 2/3, 4/5, 6/7\}$, which corresponds to mean cloning cascade lengths equal: 2, 4, 6, and 8, respectively. We can observe that, even with a low number of users, P2Priv achieves results close to the maximum in this distributed service scenario and it is robust against a high fraction of compromised nodes.

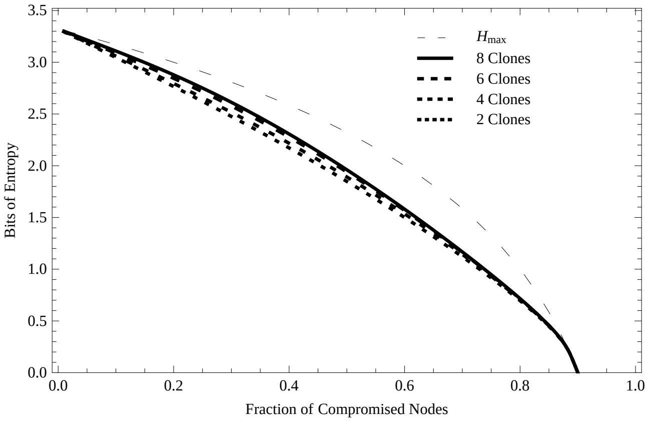


Fig. 2: Entropy for P2Priv in P2P Scenario as compared with maximum entropy, $|N| = 10$.

Figure 3 investigates the robustness of P2Priv in a large scale network comprised by $|N| = 10^3$ nodes. We observe high entropy for a low-to-medium fraction of compromised nodes.

4.2 P2Priv in Client-Server Scenario

Let us apply the P2Priv architecture to the opposite, centralized service scenario. In this case, all user nodes N connect to a single server to receive a particular content, which is an *item of interest* of the adversary. We take into account that this server is an easy target for observation and then assume that all its up-link and down-link traffic is being eavesdroped on by the adversary.

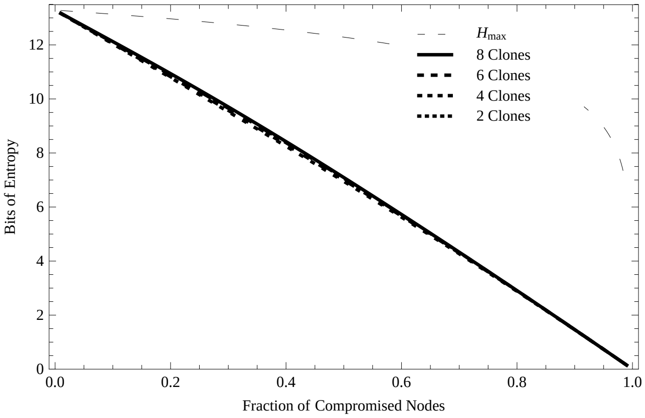


Fig. 3: Entropy for P2Priv in P2P Scenario as compared with maximum entropy, $|N| = 10^3$.

Single Request to Server. Similarly to previously analyzed attack scenario, we assume an active adversary who is able to break cloning cascade CC using fraction ρ of malicious nodes scattered in N. Summing it up, we can stress that in this case, after an initiation of a content connection to the server by *Alice*, all associated connections will be established with the server and eavesdropped on by the adversary. Then, the number of all suspected nodes can be limited by the adversary to $|CC_{break}|$ (4). The adversary knows that one of these nodes belongs to *Alice*, each of them with the probablity $p_{a1} = |CC_{break}|^{-1}$ (6). Then, entropy of P2Priv in Client-Server Scenarios is described as follows

$$\mathcal{H}_{\mathrm{p2priv/cs}} = - \sum_{k=1}^{|CC_{break}|} p_{a1} \log_2(p_{a1}) = \log_2(|CC_{break}|). \tag{10}$$

Figure 4 and Figure 5 show entropy of P2Priv architecture applied for Client-Server services. To allow an easier comparison between results obtained for small and large scale networks, the range of entropy plotted in Figure 5 is the same as in Figure 4. Then, it does not include plot for maximum entropy $\mathcal{H}_{\max}$ which certainly is the same as presented in Figure 3. As we expected, the results obtained in Client-Server Scenario are much worse than those obtained in P2P environment for which P2Priv was intended. Entropy of P2Priv architecture in centralized network is independent of the network scale for a low-to-medium compromised network and value about 1.5 bits for 10%-20% fractions of malicious nodes.

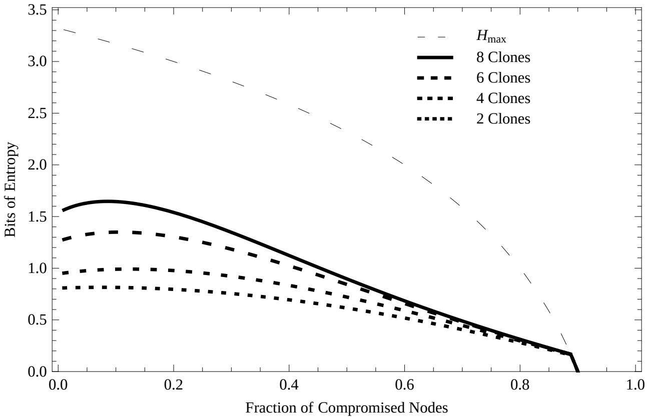


Fig. 4: Entropy for P2Priv in Client-Server Scenario as compared with maximum entropy, $|N| = 10$.

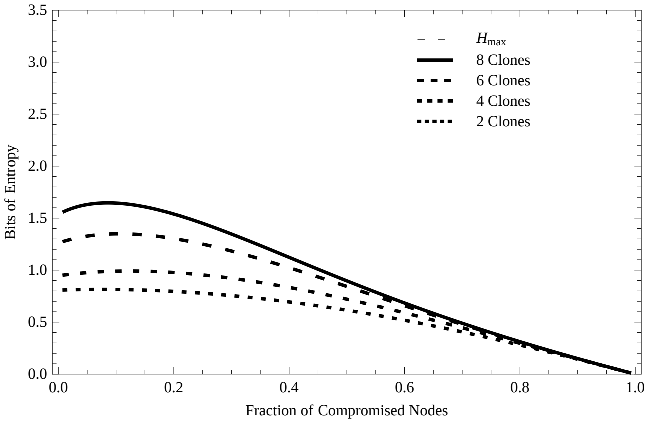


Fig. 5: Entropy for P2Priv in Client-Server Scenario, $|N| = 10^3$.

Long-Term Observation. The previous analysis shows entropy of P2Priv in centralized service scenario and the evaluated information leaks correspond to a single connection to the server. However, considering client-server services, sequential requests to a particular server are common. It should be noticed, that P2Priv does not assure long-term availability of individual nodes, so the CC is deemed to change over time (with the exception of the true sender). P2Priv was not designed for services characterized by a sequential communication to a single network node and it cannot be applied for these purposes in its current form.

4.3 Summary of the Results

We have found that the parallel transport architecture of P2Priv does not assure a satisfactory anonymity level for centralized services. Still the concept of transport parallelization and the moving of time-consuming anonymization techniques to signalization layer seem to be very attractive in the terms of anonymous traffic latency. In the rest of this paper we will discuss the possibilities of using the parallelism-based approach to network anonymization not limited to P2P content distribution.

5 Network Privacy Preserving Parallel Topology

Considering general purpose anonymous networks, we can distinguish four basic types of network nodes : (i) client/user nodes, (ii) middle-man nodes or proxy servers, (iii) the so called exit nodes, and (iv) service nodes/servers. Client nodes send requests through middle-man nodes to gain an anonymous access to services provided by service nodes (iv). On the other hand, exit nodes (iii) are middle-man nodes which are permitted by their policy to be boundary nodes of forwarding cascades—these nodes connect directly to service nodes (iv) on behalf of users (i). In various networks these sets are merged in different combinations. In particular, all nodes of pure P2P networks can act as client nodes (i), middle-man nodes (ii), exit nodes (iii), and server nodes (iv) as necessary. Such division of roles corresponds to P2Priv. However, when it comes to a generic traffic anonymization, we should separate user nodes from exit nodes as not every user wishes to commit to sharing his/her node as an exit node. Certainly, having in mind client-server network applications, we should also distinguish service nodes (iv).

To provide general-purpose sender anonymization we propose an anonymous network architecture which joins P2Priv parallel transportation of content (collective is comprised by parallel links, similary to P2Priv) with proxy functions (each link is terminated by exit node). The new architecture is derived from P2Priv P2P network and is dedicated to general-puprose anonymous networks, though it will be referred to as NetPriv (network privacy preserving parallel topology).

Let us group nodes in the anonymous network as follows: N is the set of user nodes, potential initiators of communication and E represents exit-nodes. We joined (i) and (ii) in our network model as the anonymity of the proposed solution is basically based on the difficulty of differentiation between real senders and other nodes which simultaneously act the same way the senders act. NetPriv is a hybrid solution which largely reflects P2Priv topology of parallel links between N nodes. However, each of these links is additionally terminated by a link to a mixing exit node (E). Figure 6 illustrates the model of the proposed network. In addition, it compares it to classical anonymous networks.

To allow an anonymous communication in the described architecture we propose the following sub-solutions: (i) persistent CC path selection by sender, (ii) time synchronization of requests sending by CC members.

Persistent CC Path Selection. The discussion included in Section 4.2 shows that the parallel architecture of P2Priv, considered in the scope of services characterized by series of user requests to the same destination node or server, is not robust against long-term observations. The reason is that path selection based on a random-walk does not ensure persistent CC paths, so the CC is deemed to change over time (with the exception of the true sender). The anonymity of CC communications was from the beginning assured by the Mix-net layer. Having this in mind, we propose a replacement of random-walk-based path selection for CC with free-route routing dedicated for Mix-network [1,12]. In this way a sender selects one CC for a whole session of an anonymous communication.

Requests Time Synchronization. The second issue the requires revision is answering the question how exactly CC members randomly delay their connections to destination node/nodes. To assure that the adversary can not distinguish *Alice* from other CC members by an analysis of connection times of individual clones (clone that most frequently connects first can be distinguish as the initiator), we propose inclusion of time field in cloning token which specify starting time for connections and allows synchronization of connection times. The time interval, indicated by *Alice*, should be longer than time required to send token via CC. Then, each CC member adds additinal randomly generated delay to time indicated in received token and on time calcucated in such a way he sends request to an exit node. Accordingly, cloning token will consist of the following fields:

$$\{dest\_addr, reqest\_time, request\}$$

and the request originated to a mixing exit node consists of:

$$\{src\_addr, dest\_addr, request\}_{PK_e}.$$

An exit node sends request to a destination node or nodes, based on information included in the received request. Certainly, a source address in his request pointes at him.

6 Anonymity Analysis for NetPriv

Let us analyze anonymity of the new architecture. Previously, we have shown that the parallel transport architecture assures high entropy for distributed ser-

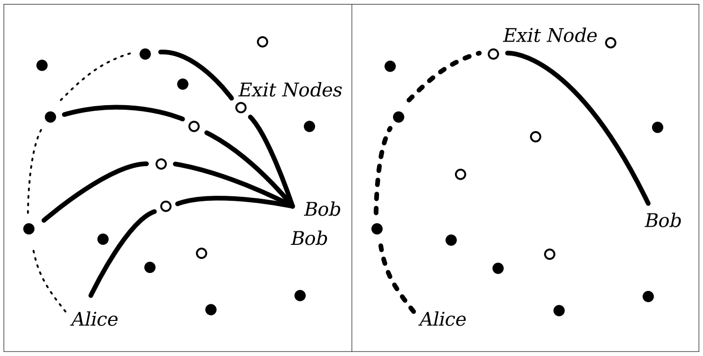


Fig. 6: NetPriv architecture (*left*) as compared to general-purpose classical anonymous network (*right*).

vices of file-sharing (8) without improvements proposed in NetPriv. The vital question is how the new architecture of NetPriv deals with Client-Server Service Scenarios (compare to Section 4.2). As the exit nodes and the user nodes have been disjointed, NetPriv anonymity model can allow an analysis of a different fraction of compromised nodes in each of these sets. One can imagine that different service scenarios provoke and permit for different collaboration possibilities, especially as it comes to the set of exit nodes which can be, e.g., dedicated servers of a particular anonymous service, public proxies, or nodes voluntarily provided by network users. As previously assumed ρ represents fraction of macilious user nodes. Let ρ_e represent fraction of malicious nodes among exit nodes. Then

$$|CC_{eavesdrop}| = \rho_e \, |CC_{break}| \, . \tag{11}$$

Similarly to the previous model, the adversary can assign probability $p_{a1}$to each node of this set (6). *Alice* can aslo be outside of eavesdropped nodes. We assume that destination nodes/servers are compromised and ρ_e of exit nodes is compromised. Then each honest node of N nodes can be *Alice* with probability

$$p_{a3} = (1 - \frac{|CC_{eavesdrop}|}{|CC_{break}|})\frac{1}{N - \rho N - |CC_{eavesdrop}|}. \tag{12}$$

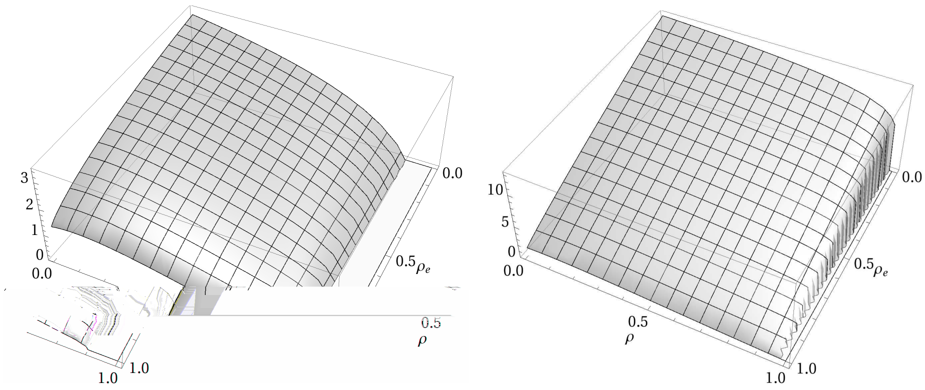
Finally, the anonymity of the NetPriv architecture in the Client-Server scenario is described by entropy

$$\begin{aligned}\mathcal{H}_{NetPriv} = & - |CC_{eavesdrop}| \, p_{a1} \log_2(p_{a1}) - \\ & (N - \rho N - |CC_{eavesdrop}|) p_{a3} \log_2(p_{a3}),\end{aligned} \tag{13}$$

$$\mathcal{H}_{NetPriv} = \frac{|CC_{eavesdrop}|}{|CC_{break}|} \log_2(|CC_{break}|) -$$

$$(1 - \frac{|CC_{eavesdrop}|}{|CC_{break}|}) \log_2 (\frac{|CC_{break}| - |CC_{eavesdrop}|}{|CC_{break}|\,(N - \rho N - |CC_{eavesdrop}|)}) \quad (14)$$

Figure 7 shows entropy of NetPriv in the full spectrum of compromised user nodes (ρ) and compromised exit nodes (ρ_e) for client-server services.



(a) $|N| = 10$

(b) $|N| = 10^3$

Fig. 7: Entropy for NetPriv architecture, $|CC| = 4$.

We can observe that the new architecture assures high entropy both for small as well as large scale networks. Exit nodes can be particularly vulnerable to being compromised. Figures 8, 9 show entropy for NetPriv for constant value of $\rho_e = 1/2$. The results show that even for this high fraction of collaborating exit nodes NetPriv assure high level of anonymity.

7 Conclusions and Future Work

Today's topologies of anonymous networks shape anonymous communications into hard to trace paths hiding their origin or destination. Transportation of anonymous content via pervasive paths composed of several hops is in favour of anonymity. Still, it imposes a significant traffic bottleneck. The phenomenon of the Internet virtualization and practical possibilities that allow us today to deploy heterogeneous overlay networks of the world-wide range encourage consideration of new network topologies adapted to specific network services. In this paper we have proposed a framework of a novel architecture for anonymous networks—the network privacy preserving parallel topology (NetPriv). NetPriv hides initiators of communications by parallelization of anonymous links. The new approach is based on the premise of the anonymous P2P network called P2Priv [16]. Contrary to P2Priv, the new architecture can be suited to the anonymization of general-purpose network communications. The new solution

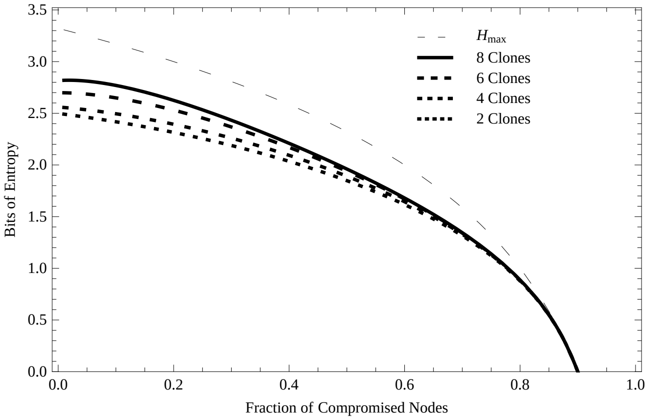


Fig. 8: Entropy for NetPriv in Client-Server Scenario as compared with maximum entropy, $|N| = 10$.

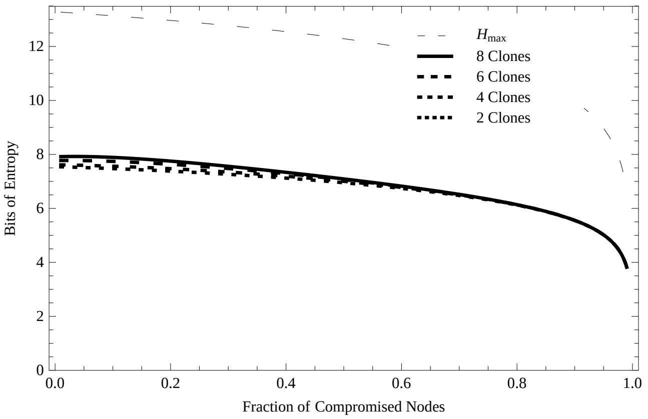


Fig. 9: Entropy for NetPriv in Client-Server Scenario as compared with maximum entropy, $|N| = 10^3$.

moves time-consuming anonymization techniques into a signalization layer and combines the primary transport parallelization principle of P2Priv with proxy functions. Additionally, a persistent selection of signalization paths and requests time synchronization mechanisms have been proposed. We applied an information theoretic entropy measurement model to evaluate anonymity of both architectures. We analyzed anonymity of the previous (P2Priv) and the new (NetPriv) architectures with a particular emphasis on centralized, client-server service scenarios. We have found that P2Priv can assure high degree of anonymity in the limited scope of network services. P2Priv is dedicated to a large size content distribution and requires a distributed service overlay network to assure high degree of anonymity. Additionally, we have found that anonymity of P2Priv decreases when destination points of communication are not distributed. Contrary to the previous solution, we have found that the new architecture can be applied to the anonymization of various network communications, including client-server services (e.g., anonymous Web access). For a realistic scope of compromised network nodes, NetPriv anonymity is close to maximum. From the user's point of view, the new solution offers a high level of anonymity within only a single proxy node.

The new parallelism-based approach presented in this paper gives the framework for parallel anonymous topologies. However, it should be noticed that this discussion encourages further work. The first vital issue, that needs to be addressed, is the design of follow-up extensions allowing for a bi-directional anonymous communication which includes a receiver anonymity. Secondly, an interesting area of NetPriv analysis is its traffic performance evaluation. Certainly, NetPriv, which allows anonymous transportation via a single proxy, can be considered as the solution able to significantly improve the speed of an anonymous communication (the traffic analysis of P2Priv demonstrates substantial decreases of the content transportation time as compared with traditional networks [16,17,15]). However, a detailed and practical analysis can be helpful in determination of proper NetPriv configurations and its exact impact on network traffic.

References

1. Oliver Berthold, Andreas Pfitzmann, and Ronny Standtke. The disadvantages of free mix routes and how to overcome them. In H. Federrath, editor, *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, pages 30–45. Springer-Verlag, LNCS 2009, July 2000.
2. Rainer Böhme, George Danezis, Claudia Diaz, Stefan Köpsell, and Andreas Pfitzmann. Mix cascades vs. peer-to-peer: Is one concept superior? In *Privacy Enhancing Technologies (PET 2004)*, 2004.
3. Jan Camenisch and Anna Lysyanskaya. A formal treatment of onion routing. In Victor Shoup, editor, *Proceedings of CRYPTO 2005*, pages 169–187. Springer-Verlag, LNCS 3621, August 2005.
4. David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 4(2), February 1981.

5. Lance Cottrell. Mixmaster and remailer attacks, 1994.
6. George Danezis. Mix-networks with restricted routes. In Roger Dingledine, editor, *Proceedings of Privacy Enhancing Technologies workshop (PET 2003)*, pages 1–17. Springer-Verlag, LNCS 2760, March 2003.
7. George Danezis and Bettina Wittneben. The economics of mass surveillance and the questionable value of anonymous communications. In Ross Anderson, editor, *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006)*, Cambridge, UK, June 2006.
8. Claudia Diaz, Len Sassaman, and Evelyne Dewitte. Comparison between two practical mix designs. In *Proceedings of ESORICS 2004*, LNCS, France, September 2004.
9. Claudia Diaz, Stefaan Seys, Joris Claessens, and Bart Preneel. Towards measuring anonymity. In Roger Dingledine and Paul Syverson, editors, *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002)*. Springer-Verlag, LNCS 2482, April 2002.
10. Roger Dingledine and Nick Mathewson. Anonymity loves company: Usability and the network effect. In Ross Anderson, editor, *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006)*, Cambridge, UK, June 2006.
11. Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, pages 303–320, San Diego, CA, USA, August 2004.
12. Roger Dingledine, Vitaly Shmatikov, and Paul Syverson. Synchronous batching: From cascades to free routes. In *Proceedings of Privacy Enhancing Technologies workshop (PET 2004)*, volume 3424 of *LNCS*, pages 186–206, May 2004.
13. David M. Goldschlag, Michael G. Reed, and Paul F. Syverson. Hiding routing information. In R. Anderson, editor, *Proceedings of Information Hiding: First International Workshop*, pages 137–150. Springer-Verlag, LNCS 1174, May 1996.
14. Ceki Gülcü and Gene Tsudik. Mixing e-mail with babel. In *Proceedings of the Network and Distributed Security Symposium - NDSS '96*, pages 2–16. IEEE, February 1996.
15. Igor Margasinski. *Anonymous Transport in Peer-to-Peer Overlay Networks.* PhD thesis, Warsaw University of Technology, June 2008.
16. Igor Margasinski and Michal Pioro. A concept of an anonymous direct p2p distribution overlay system. In *Proceedings of IEEE 22nd International Conference on Advanced Information Networking and Applications (AINA)*, pages 590–597, Gino-wan, Okinawa, Japan, March 2008. IEEE Computer Society Press.
17. Igor Margasinski and Michal Pioro. Low-latency parallel transport in anonymous peer-to-peer overlays. In et al. N. Akar, editor, *IP Operations and Management*, volume LNCS 5275, pages 127–141. Springer Berlin / Heidelberg, 2008.
18. Michael Reiter and Aviel Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*, 1(1), June 1998.
19. Andrei Serjantov and George Danezis. Towards an information theoretic metric for anonymity. In Roger Dingledine and Paul Syverson, editors, *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002)*. Springer-Verlag, LNCS 2482, April 2002.